学校编码：10384　　分类号____密级____
学号：23120091152685　　UDC_____

厦门大学

硕 士 学 位 论 文

基于哈希引擎的安全器件的设计研究

Design and Implementation of safe device based on hash

奎伟

指导教师姓名： 周剑扬　副教授
专 业 名 称： 微电子学与固体电子学
论文提交日期： 2012 年　月
论文答辩时间： 2012 年　月
学位授予日期： 2012 年　月

答辩委员会主席：_____
评　　阅　　人：_____

2012 年　月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘　要

随着现代技术的飞速发展，社会的信息化应用不断向前推进。互联网，通信和计算机系统的开放程度越来越高，在高度互联的通信和计算机系统中, 维护信息安全，建立安全可靠的电子信息网络，无论对国家还是对个人都是非常重要的。

维护信息安全，意味着我们要通过加密的方法对客户的有关信息如密码、合同等加以保护, 使之不被盗取或篡改。而当客户提出服务申请时, 必须对客户身份的合法性、报文的完整性进行确认，防止非法复制程序代码和重要数据，避免数据或代码被非法修改，保护电子交易。

哈希函数作为单向散列函数，具有很好的加密特性。哈希加密在身份验证和数据完整性，以及网络信息安全方面得到了较好的应用和实现。譬如：软件代码保护、软件授权和升级管理、配件识别和电子标签、网上身份识别、电子钱包、数据传输和媒体文件的加解密, 以及 DVB、STB 和 CMMB 的条件接受系统等应用。基于哈希加密验证的原理，研发出了哈希安全器件，能够防止信息泄露和篡改，从低成本的角度保护用户的数据安全。

本文首先分析了数字安全加密算法的发展及其在相关信息安全领域中的应用情况，接着详细阐述了 SHA1、SHA256、SHA384、SHA512 等系列算法的分类，原理和计算过程，并进行了比较。接下来基于硬件开发环境和相关编程语言，从硬件角度选择并实现了 SHA256 加密算法，同时运用循环展开，预计算等方法，对算法优化进行了讨论。通过 Modelsim 仿真，ISE 综合验证以及相关数据的分析对比，对算法优劣进行了评价和总结。

接下来从系统的角度，提出了带 SHA-256 引擎的 1K 位安全存储器 EEPROM 的架构。其中分析了 I2C 协议，EEPROM 各部分寄存器功能，并对安全器件的工作原理和数据读写、计算、双向质询、验证过程进行了讨论和研究。最后采用 Verilog HDL 对各个功能模块进行行为级建模，通过 Modelsim 仿真，结果表明该安全器件的结构、功能满足设计要求。

关键词：加密；算法；安全器件

Abstract

With the rapid development of modern technology, the application of information technology is progressing forward. The Internet, communication and computer system are more and more open. In the advanced Internet communication and computer system, the maintenance of information security, the establishment of safe and reliable electronic information network, are important to both national and personal.

Maintaining the information safe means that, we must protect the customer's relevant information to be stolen or tamper with the encryption method, such as the password ,contracts, etc. And when the customer come out a service application, we have to confirm the identity legitimacy of the client, or the integrity of the message,in order to prevent the illegal copying the program code and important data, and avoid the illegal modification of data and the code, so as to protect the electronic trading.

As a one-way hash function, Hash function has the very good encryption characteristic. Hash encryption has the excellent application and implementation in the identity authentication and data integrity, and the network information security. For example: software code protection, software license and upgrade management, fitting recognition and electronic label, online identity recognition, electronic purse, data transmission and media file encryption, and DVB, STB and CMMB system applications. Based on the hash encryption principle, we developed the hash safety device, which can prevent information leakage and manipulation, protect the user's data security with low cost.

This paper first analyzes the development of the encryption in the digital security and the application in the related information security fields, then elaborate the algorithm principle, classification and calculation process of SHA1, SHA256, SHA384, SHA512, then compare with them. Based on the hardware development environment and related programming languages, we realize SHA256 encryption algorithm in the hardware way. At the same time, we use the loop unrolling, pre-calculating methods to optimize the algorithm. Through the Modelsim and ISE

tools, and the data from the simulation and synthesize, we analyze the quality of the algorithm.

Then we propose a eigneering design of safety device with SHA-1 engine, which contain 1k bit EEPROM memory. Then we analyze the principle of I2C, the function of each register in the EEPROM, the working principle of the safe device, the reading and writing data way, the calculation, two-way inquiry, verification process and so on. Finally we use Verilog HDL to model the each function module, through the Modelsim simulation, we know that the structure, function of the safety device meet the design requirements.

Keywords: Encryption; Algorithm,Safety device

目 录

Contents